JOURNAL OF NUMBER THEORY 5, 390–404 (1973)

Invariants for Quadratic Forms

J. H. CONWAY

Department of Pure Mathematics and Mathematical Statistics,
University of Cambridge, Cambridge CB2 1SB, England

PRESENTED AT THE QUADRATIC FORMS CONFERENCE, BATON ROUGE, LOUISIANA, MARCH 27–30, 1972,
AND DEDICATED TO THE MEMORY OF LOUIS JOEL MORDELL

Simple systems of invariants for rational and integral quadratic forms are given, and those for rational forms are proved complete in an elementary way. Some noninvariants of quadratic forms appear, but we are not concerned with invariants of objects other than quadratic forms. Our treatment of noninvariants of objects other than quadratic forms is minimal, and it is here that there is most room for further investigation.

The object of this note is to produce, first, complete systems of invariants for rational quadratic forms and the genera of integral quadratic forms, and second, a simple proof of completeness for the rational invariants. I wish to make it clear at the outset that the invariants for integral forms were produced by "digesting" the invariants and canonical forms given in papers of Gordon Pall and Burton Jones, so that I do not purport to give independent proofs of their invariance or completeness.

The invariants for rational forms (though not the proof of their completeness) generalize naturally to give similar invariants for forms over any global field, and in particular, any algebraic number field. Similarly, the invariants for rational integral forms generalize to give similar but more complicated invariants for forms over algebraic integers. Again, no independent proof of invariance or completeness is envisaged, the generalized invariants being produced simply by "digesting" those in the book of O'Meara.

The idea is to examine these invariants to find the structure of the semigroup they define at each Jordan component, and then to investigate the possibility of passing part of the structure from one component to the next (or in more general fields, of "catalyzing" one component by some property of its neighbor). It is an essential feature of the method that one does *not* aim at a single-valued invariant, but rather one whose many values are easily transformed into one another. It seems somewhat

arbitrary to pick upon just one of these values as canonical, and any rule for doing so adds considerable extra complication. (Indeed, it is only this which makes the unique-valued invariants of Gordon Pall, or the unique canonical form of Burton Jones, so much more complicated to work with.)

I have tried to make the paper useful to mathematicians whose interests are mainly in other fields, and to ensure that a reader interested only in the practical calculation of the invariants can isolate what he needs without reading all of the paper. For this reason, I have avoided the p-adic numbers (though not the term "p-adic") in the first part of the paper, and made only minor uses of them in the remainder. I have also concentrated on producing a compact symbol which should contain all the desired information about a given quadratic form.

Rational Forms

A rational form can be diagonalized by a rational transformation. This amounts essentially to the familiar process of "completing the square"—thus, the form

$$ax^2 + 2bxy + 2cxz + \cdots + \text{terms involving only } y, z, \ldots$$

can be written as

$$a^{-1}(ax + by + cz + \cdots)^2 + \text{terms involving only } y, z, \ldots$$

if a is nonzero, so that in terms of the new variables

$$x' = ax + by + cz + \cdots, \qquad y' = y, \qquad z' = z, \ldots$$

it has become the sum of a form involving only x' and another involving only $y', z', \ldots$ (a sum of forms in disjoint variables is called a *direct* sum). Repeating the process, we eventually arrive at a diagonal form (direct sum of one-dimensional forms)

$$AX^2 + BY^2 + \cdots$$

unless at some stage we have a summand in which all the diagonal coefficients are zero, but there is some other nonzero term, $2ky'z'$, say. But in this case we can produce a nonzero diagonal term by changing to new variables $y'' = y' + z'$, $z'' = z', \ldots$.

In terms of the matrix of the form we accomplish these transformations by adding or subtracting multiples of one row from the others, followed immediately by the corresponding column operations, in any way so that ultimately all the off-diagonal entries become zero. Thus matrix B

below is obtained from A by subtracting twice the first row from the second,

A			B			C			D		
1	2	3	1	2	3	1	0	0	1	0	0
2	4	5	0	0	−1	0	0	−1	0	1	2
3	5	6	0	−1	−3	0	−1	−3	0	−1	−3

E			F			G		
1	0	0	1	0	0	1	0	0
0	−1	2	0	−1	2	0	−1	0
0	2	−3	0	0	1	0	0	1

and thrice this row from the third, and C is obtained from B by the corresponding column operations. Then C yields D on subtracting the third row from the second, and D becomes E on subtracting the third column from the second. Finally, we obtain F by adding twice the second row of E to the third, and G from F by the corresponding column operation. (In this example we have used unnecessarily many operations so as to avoid the appearance of fractions.)

So we need deal only with diagonal rational forms, writing $\langle a, b, c,... \rangle$ for the form $ax^2 + by^2 + cz^2 + \cdots$. Since we can multiply the entries by nonzero rational squares, we can further suppose them to be square-free integers, if we like. We shall almost always suppose further that the form is *nondegenerate*, i.e., $d = abc \cdots \neq 0$.

The Rational Invariants

We say that two numbers are in the same *rational square-class* if their product is a nonzero rational square. Thus, the square-free numbers are representatives of the rational square-classes. If p is one of the prime numbers 2, 3, 5,..., we shall say that two nonzero numbers are in the same *p-adic square-class* if their product is congruent to a square modulo arbitrarily high powers of p (equivalently, is the square of a p-adic rational number). Finally, we introduce "the infinite prime" ∞, and say that two numbers are in the same *∞-adic square-class* if their product is positive (i.e., the square of a nonzero *real* number). Then representatives of the p-adic square-classes are the numbers x in the table, which also defines the function $[x]_p$, constant on each p-adic square-class:

	$p = \infty$	$p = 2$	$p = 4k + 3$	$p = 4k + 1$
x:	1 −1	1 −1 5 −5 2 −2 10 −10	1 −1 p $-p$	1 u p up
$[x]_p$:	1 i	1 $-i$ 1 $-i$ 1 $-i$ −1 i	1 1 i $-i$	1 1 1 −1

We define the numbers n_+, n_- for the quadratic form $f = \langle a, b, c, \ldots \rangle$ to be the numbers of positive and negative terms among $a, b, c, \ldots$, respectively.

THEOREM 1. *The following are a complete system of rational invariants for the form f:*

(i) *The numbers n_+, n_-, and the rational square-class of the determinant $d = abc \cdots$.*

(ii) *The numbers $[f]_p = [a]_p [b]_p [c]_p \cdots$ for each prime $p = 2, 3, 5, \ldots, \infty$.*

This theorem will be proved at the end of the paper. The proof will be entirely self-contained, whereas it does not seem possible to prove our next theorem without appeal to some principle from outside the theory of rational forms. Traditionally one *either* supposes with Legendre that each arithmetic progression contains an infinity of primes *or* follows Gauss in deducing the corresponding theorem first for integral forms.

THEOREM 2. *Suppose for each $p = 2, 3, 5, \ldots, \infty$ we have a form f_p of determinant d. Then there exists a form f with $[f]_p = [f_p]_p$ for each p, and with the same n_+, n_-, as f_∞ if and only if we have the product formula:*

$$[f_\infty]_\infty \cdot [f_2]_2 \cdot [f_3]_3 \cdots = 1.$$

In other words essentially the only relationship between the invariants $[f]_p$ for differing p is the condition that their product over all p be 1. The product is meaningful because in fact $[f]_p = 1$ for all finite primes not dividing $2d$. Since it is easy to see when forms f_p exist for each p, the theorem gives necessary and sufficient conditions for there to exist a form with prescribed invariants.

INTEGRAL FORMS

We shall say that every real number is *∞-adically integral*, and that a rational number is *p-adically integral* if the finite prime p does not divide its denominator. There are corresponding notions of p-adically integral transformations, in which all the numbers involved (as matrix-entries) are required to be p-adically integral. For all $p \neq 2$ our previous proof shows that an integral form can be diagonalized by a p-adically integral transformation—we simply look for terms divisible by the least possible power of p instead of nonzero terms.

However, for $p = 2$ the best we can do is express the form as a direct sum of one- and two-dimensional forms, the latter all being of the form $\left[\begin{smallmatrix} qa & qb \\ qb & qc \end{smallmatrix}\right]$, where q is a power of 2, and a and c are odd, b even. To see this, we let q be the least power of 2 dividing all entries in the remaining part of the form. If some diagonal term is not divisible by $2q$, we proceed as before. If not, there is a submatrix $\left[\begin{smallmatrix} qa & qb \\ qb & qc \end{smallmatrix}\right]$ of the above kind, and we can subtract suitable multiples of the rows and columns of this matrix from the others so as to make it into a direct summand. Thus, in matrix A the required submatrix is $\left[\begin{smallmatrix} 2 & 1 \\ 1 & 4 \end{smallmatrix}\right]$, and we

$$\begin{matrix} 2 & 1 & 3 & 0 \\ 1 & 4 & 5 & 7 \\ 3 & 5 & 6 & 9 \\ 0 & 7 & 9 & 8 \end{matrix} \qquad \begin{matrix} 2 & 1 & 3 & 0 \\ 1 & 4 & 5 & 7 \\ 0 & 0 & -2 & 2 \\ 0 & 0 & 2 & -6 \end{matrix} \qquad \begin{matrix} 2 & 1 & 0 & 0 \\ 1 & 4 & 0 & 0 \\ 0 & 0 & -2 & 2 \\ 0 & 0 & 2 & -6 \end{matrix}$$

A B C

$$\begin{matrix} 2 & 1 & 0 & 0 \\ 1 & 4 & 0 & 0 \\ 0 & 0 & -2 & 2 \\ 0 & 0 & 0 & -4 \end{matrix} \qquad \begin{matrix} 2 & 1 & 0 & 0 \\ 1 & 4 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & -4 \end{matrix}$$

D E

subtract the sum of its rows from the third row, and add then the first and subtract twice the second from the last row, to get matrix B. Matrix C is then produced by the corresponding column operations, and in the untreated part $\left[\begin{smallmatrix} -2 & 2 \\ 2 & -6 \end{smallmatrix}\right]$ of this there is a diagonal term -2 divisible by the least possible power of 2. So we add the third row to the fourth, getting matrix D, and the third column to the fourth, arriving finally at the form with matrix E. The transformation we have used is integral and, therefore, p-adically integral for all p, and it produces the final answer for $p = 2$. But for $p \neq 2$ we can go further, subtracting half the first row from the second, then half the first column from the second, to produce the diagonal form $\langle 2, 7/2, -2, -4 \rangle$.

For $p \neq \infty$, a *p-power* will mean any power of p, while *∞-power* will mean either of the numbers 1 and -1 (often abbreviated $+$ and $-$). A p-adically integral form will be called a *p-adic unit-form* if its determinant is not divisible by p (p finite), or if it is positive definite ($p = \infty$). By collecting summands in the decomposition we have found, we can express f as a direct sum of distinct p-powers times p-adic unit-forms (its *Jordan components*).

THE INTEGRAL INVARIANTS

For each p, we shall define a number of invariants associated with the various p-powers q. We write f in its *Jordan decomposition* as a direct sum of forms qf_q, in which there is one unit-form f_q for each p-power q, so that in fact almost all the f_q are zero-dimensional. Then the *q-dimension* $\dim_q(f)$ is defined to the dimension of f_q, and the *q-signum*, $\mathrm{sig}_q(f)$, by

For $p = \infty$, $\mathrm{sig}_q = 1$.
For p odd, sig_q is the Legendre symbol $(\det(f_q)/p)$.
For $p = 2$, we define first

$$\mathrm{sig}_q[qd] = \delta, i\delta, \phi\delta, i\phi\delta \text{ according as } d \equiv 1, -1, 5, -5 \pmod 8,$$

and

$$\mathrm{sig}_q \begin{bmatrix} qa & qb \\ qb & qc \end{bmatrix} = i, -i\phi \text{ according as } d = ac - b^2 \equiv -1, -5 \pmod 8.$$

(Here a, b, c, d are all 2-adically integral, with a and c even, b odd.) Then for direct sums of such forms we use the rules

$$\dim_q(f \oplus g) = \dim_q(f) + \dim_q(g), \qquad \mathrm{sig}_q(f \oplus g) = \mathrm{sig}_q(f) \cdot \mathrm{sig}_q(g)$$

and the relations $i^2 = -1$, $\phi^2 = 1$, $\delta^2 = \delta$ to multiply the signa. In all cases we have $\dim_q(f) = \dim_q(qf_q)$, $\mathrm{sig}_q(f) = \mathrm{sig}_q(qf_q)$.

THEOREM 3. *For $p \neq 2$, two forms f and g are p-adically equivalent if and only if they have the same numbers* $\dim_q$ *and* sig_q *for each p-power q, and their determinants have the same square-class. Two forms f and g are 2-adically equivalent if and only if they have the same numbers* $\dim_q$ *for each 2-power q, and if the sequence of numbers* sig_q *for f can be transformed into that for g by repeated use of the rules*:

$\mathrm{sig}_q, \mathrm{sig}_{2q}$ *may be replaced by*

$$\begin{cases} \phi\,\mathrm{sig}_q, -\phi\,\mathrm{sig}_{2q}, \text{ if } \delta \text{ divides } \mathrm{sig}_q, \\ -\phi\,\mathrm{sig}_q, \phi\,\mathrm{sig}_{2q}, \text{ if } \delta \text{ divides } \mathrm{sig}_{2q}, \\ i\,\mathrm{sig}_q, -i\,\mathrm{sig}_{2q}, \text{ if } \delta \text{ divides both } \mathrm{sig}_q \text{ and } \mathrm{sig}_{2q}. \end{cases}$$

If one signum-sequence can be transformed into another, then the transformation can be performed in ascending order of q, so that the theorem is effective. It is important to realize that the transformations in this theorem are to be performed without reference to the existence of forms having the intermediate signum-sequences for their invariants.

Now it is customary to say that two forms belong to the same *genus* if and only if they are p-adically equivalent for all p, including ∞. So the invariants we have given for all p collectively determine the genus, and we call them the *generic invariants.*

For our second example, we have, in the case $p = 2$,

$$\dim_1 = 2, \quad \mathrm{sig}_1 = i, \quad \text{since} \begin{vmatrix} 2 & 1 \\ 1 & 4 \end{vmatrix} = 7 \equiv -1 \pmod 8,$$

and

$$\dim_2 = \dim_4 = 1, \quad \mathrm{sig}_2 = \mathrm{sig}_4 = i\delta$$

from the remaining terms.

For other primes we can use the diagonal form $\langle 2, 7/2, -2, -4\rangle$ with $d = 56$, and so for $p = \infty$ we have

$$\dim_+ = \dim_- = 2, \qquad \mathrm{sig}_+ = \mathrm{sig}_- = 1,$$

for $p = 7$, we have

$$\dim_1 = 3, \quad \mathrm{sig}_1 = \left(\frac{16}{7}\right) = +1, \quad \dim_7 = 1, \quad \mathrm{sig}_7 = \left(\frac{1/2}{7}\right) = +1,$$

for all other p,

$$\dim_1 = 4, \qquad \mathrm{sig}_1 = (56/p).$$

In each case, we have $\dim_q = 0$, $\mathrm{sig}_q = 1$ for all unmentioned q.

For $p = 2$, we can successively transform the signum-sequence from

$$i, i\delta, i\delta \text{ through } -i\phi, i\phi\delta, i\delta \qquad \text{and} \qquad -i\phi, i\delta, -i\phi\delta \text{ to } -i\phi, \delta, \phi\delta,$$

which is the signum-sequence for $\left[\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right] \oplus [2] \oplus [28/3]$, so that f is 2-adically equivalent to this form. (But the 7-adic invariants of the new form are $\dim_1 = 3$, $\mathrm{sig}_1 = -1$, $\dim_7 = 1$, $\mathrm{sig}_7 = -1$, so that the two forms are *not* 7-adically equivalent.)

It is as well to notice that there is no form with $\dim_4 = 1$ and $\mathrm{sig}_4 = -i\phi\delta$, so that at an intermediate stage the sequence of numbers sig_q did not correspond to any form with the given numbers $\dim_q$. In fact it is essential for the truth of Theorem 3 that we allow arbitrary intermediate signum-sequences of this type, provided only that the initial and final sequences correspond to the forms we are considering.

It is obvious that we can compute the rational invariants from the integral ones, and for the reader's convenience we append the formula

$$[f]_p = \frac{\left(\frac{i}{p}\right)^{\dim_p + \dim_{p^3} + \cdots}}{\mathrm{sig}_1^+ \cdot \mathrm{sig}_p^- \cdot \mathrm{sig}_{p^2}^+ \cdot \mathrm{sig}_{p^3}^- \cdots},$$

where (i/p) denotes i for $p = \infty$ or $4k + 3$, and 1 for $p = 2$ or $4k + 1$, and $\mathrm{sig}^- = \mathrm{sig}$, $\mathrm{sig}^+ = 1$ for $p \neq 2$, while for $p = 2$, $\mathrm{sig}^\pm$ is obtained from sig by writing $\delta = 1$, $\phi = \pm 1$.

Then complementing Theorem 3 we have an analog of Theorem 2.

THEOREM 4. *If we have for each p a form f_p with discriminant d ($p = 2, 3, \ldots, \infty$), then there will exist a single integral form f with the same p-adic invariants as f_p for each p if and only if we have the product formula*

$$[f_\infty]_\infty \cdot [f_2]_2 \cdot [f_3]_3 \cdots = 1.$$

Since it is easy to see when there is a form with prescribed p-adic invariants for any one p, the theorem gives necessary and sufficient conditions for there to exist a form with prescribed generic invariants.

THE p-ADIC AND GENERIC INDICATORS

We describe a convenient way of specifying all the generic invariants at a glance. We start from the observation that the formal product $\text{ind}_q = \dim_q \cdot \text{sig}_q$ determines both the numbers $\dim_q$ and sig_q, because *either* $\dim_q$ is a positive integer, *or* $\dim_q = 0$, $\text{sig}_q = 1$. (This is not so at intermediate stages in the transformation process for $p = 2$, and so we must not use generic indicators in those transformations.) It is convenient to write $|i| = |-1| = |\phi| = |\delta| = 1$, so that $\dim_q = |\text{ind}_q|$. We call the "number" $\text{ind}_q = \text{ind}_q(p)$ the *q-index* of the form for the prime p, and, of course, we need only specify p when $q = 1$.

Now we define the *full p-adic indicator* of f to be the formal product of symbols $q^{\text{ind}_q(p)}$ over all p-powers q, omitting any terms q^0. We obtain the ordinary *p-adic indicator* by omitting the term for $q = 1$, except that for $p = 2$ we define the ordinary p-adic indicator to be the same as the full p-adic indicator.

In our example, with $p = 2$, we have $\text{ind}_1 = 2i$, $\text{ind}_2 = \text{ind}_4 = i\delta$, and other $\text{ind}_q = 0$, so that the 2-adic indicator is the formal symbol

$$1^{2i}2^{i\delta}4^{i\delta}.$$

Similarly the full ∞-adic indicator is $(+)^2(-)^2$, and the full 7-adic indicator 1^37^1. In this example, the only nonempty p-adic indicators are

$$1^{2i}2^{i\delta}4^{i\delta},\ (-)^2,\quad \text{and}\quad 7^1$$

corresponding to $p = 2$, ∞, and 7.

For $p \neq 2$, the 1-index is determined by the other q-indices together with the determinant and dimension of the form, so that in general we can specify the p-adic equivalence class by giving these invariants together with the p-adic indicator. But since each nonempty p-adic indicator determines its prime p, we can define *the generic indicator* to be the

formal product of *all* the p-adic indicators. So the generic indicator of our example is simply

$$(-)^2 1^{2i} 2^{i\delta} 4^{i\delta} 7.$$

This remarkably short symbol in fact captures *all* the generic invariants, for the determinant is the product of all factors $q^{|\mathrm{ind}_q|}$, and the dimension is $|\mathrm{ind}_1| + |\mathrm{ind}_2| + |\mathrm{ind}_4| + \cdots$. From the generic indicator, most of the interesting properties of the form can be read off at a glance. But we must remember that the signa $\mathrm{sig}_1, \mathrm{sig}_2, \mathrm{sig}_4, \ldots$ are not completely invariant, but only to within the transformations of Theorem 3, which for safety's sake should not be performed in terms of the generic indicator.

The Theory of Rational Equivalence

The more general part of this theory applies to any field $\mathbf{F}$ not of characteristic 2, in particular, to the fields $\mathbf{R}$ and $\mathbf{Q}_p$ of real numbers and rational p-adic numbers as well as the familiar field $\mathbf{Q}$ of rational numbers. We write $f =_{\mathbf{F}} g$ to mean that f and g are equivalent under a transformation with coefficients in $\mathbf{F}$ (not of characteristic 2). The reader who is not familiar with the p-adic numbers should read first the proofs of Witt's theorem and of the completeness of the invariants, where they do not appear. We have not thought it worth while to suffer the circumlocutions involved in avoiding their use in the proof of invariance.

Binary Forms

THEOREM 5. *Two binary forms of the same determinant are equivalent over* $\mathbf{F}$ *if and only if there is some nonzero number represented by both.*

Proof. If f of determinant d represents $a \neq 0$ at the vector x, x can be chosen as the first member of a diagonal base, and so

$$f \underset{\mathbf{F}}{=} \langle a, d/a \rangle \underset{\mathbf{F}}{=} \langle a, da \rangle.$$

FIRST COROLLARY. $[f]_p$ *is an invariant for p-adic rational equivalence (and so for rational equivalence) of binary forms.*

Proof. It is easy to verify the following table, which shows how the value of $[f]_p$ can be determined from the p-adic square-classes represented by f.

	Square-classes represented by f				Square-classes represented by f				
	d	$[d]_p$	if $[f]_p = [d]_p$:	if $[f]_p = -[d]_p$:	d	$[d]_p$	if $[f]_p = [d]_p$:	if $[f]_p = -[d]_p$:	
	1	1	1	-1					
$p = \infty$	1	-1	all	none	1	1	$1, -1$	$p, -p$	
					-1	1	all	none	
	1	1	1, 5, 2, 10	$-1, -5, -2, -10$	p	i	$1, p$	$-1, -p$	$p = 4k + 3$
	-1	$-i$	all	none	$-p$	$-i$	$1, -p$	$-1, p$	
	5	1	$1, 5, -2, -10$	$-1, -5, 2, 10$					
	-5	$-i$	$1, -1, 5, -5$	$2, -2, 10, -10$	1	1	all	none	
$p = 2$	2	1	$1, -5, 2, -10$	$-1, 5, -2, 10$	u	1	$1, u$	p, up	
	-2	$-i$	$1, -1, 2, -2$	$5, -5, 10, -10$	p	1	$1, p$	u, up	$p = 4k + 1$
	10	-1	$1, -5, -2, 10$	$-1, 5, 2, -10$	up	-1	$1, up$	u, p	
	-10	i	$1, -1, 10, -10$	$5, -5, 2, -2$					

Here "all" means that all numbers including zero have nontrivial representations, and "none" means that no such form exists. In general zero has a nontrivial representation (i.e., the form is *isotropic*) only when the determinant has the squareclass of -1, when the form is equivalent to $\langle 1, -1\rangle$ and represents all numbers. See the second corollary.

SECOND COROLLARY. $\langle n, -n\rangle =_{\mathbf{F}} \langle 1, -1\rangle$, *and* $\langle 1, 1\rangle =_{\mathbf{Q}_p} \langle u, u\rangle$, *$u$ the least nonresidue of the odd prime p.*

Proof. $n(x^2 - y^2)$ and $x^2 - y^2$ both represent all numbers. $\langle 1, 1\rangle$ represents u p-adically since $u \equiv x^2 + 1 \pmod p$ for some x.

THEOREM 6 (Witt's theorem). *If* $\langle a, b, c,...\rangle =_{\mathbf{F}} \langle a, b', c',...\rangle$, *then* $\langle b, c,...\rangle =_{\mathbf{F}} \langle b', c',...\rangle$.

Proof. In a suitable inner-product space there is an orthogonal base of vectors $x, x', x'',...$, with respective norms $a, b, c,...$, and a second such base $y, y', y'',...$ with norms $a, b', c',...$. In this interpretation, the theorem asserts that there is an isometry taking $x^\perp$ to $y^\perp$. But the *reflection in z*

$$x \to x - \frac{2(x, z)}{(z, z)} \cdot z$$

is an isometry whenever $(z, z) \neq 0$, and so since at least one of $x \pm y$ has nonzero norm, there is an isometry taking x to $\mp y$, and so $x^\perp$ to $y^\perp$.

Witt's theorem immediately extends to the assertion that if f is non-degenerate and $f \oplus g =_{\mathbf{F}} f \oplus h$, then $g =_{\mathbf{F}} h$.

COROLLARY. (Sylvester's *law of inertia*) $\dim_+$ *and* $\dim_-$ *are invariants of real equivalence.*

Proof. If $\langle a, b, c,...\rangle =_{\mathbf{R}} \langle a', b', c',...\rangle$, then $a, b, c,...$ cannot all be of opposite sign to all of $a', b', c',...$, so we may suppose $a = a'$ to within a real square factor. Witt's theorem now provides us with an inductive proof.

THEOREM 7. $[f]_p$ *is an invariant of p-adic rational equivalence (and so of rational equivalence).*

Proof. After Witt's theorem it will suffice to show that two ternary forms $f = \langle a, b, c\rangle$ and $g = \langle a', b', c'\rangle$ can be made to have equal first entries by p-adic rational transformations each involving only two terms, for such do not affect $[f]_p$ by the first corollary to Theorem 5.

If p is odd, the entries are chosen from essentially just four possibilities $1, u, p, up$, where u is a nonresidue for p. If none of a, b, c is divisible by p, we can use $\langle 1, 1\rangle =_{\mathbf{Q}_p} \langle u, u\rangle$ to successively transform a to 1 and b to -1, so that f becomes $\langle 1, -1, c\rangle =_{\mathbf{Q}_p} \langle p, -p, c\rangle$. So we can suppose that each of f and f' has some entry divisible by p, and similarly some entry not divisible by p. But now we can use $\langle 1, 1\rangle =_{\mathbf{Q}_p} \langle u, u\rangle$ or $\langle p, p\rangle =_{\mathbf{Q}_p} \langle up, up\rangle$ to make f, f' have a common term.

If $p = 2$ the entries are essentially chosen from ± 1, ± 5, ± 2, ± 10, and if all are odd (even) we can use

$$\langle n, n\rangle \underset{Q}{=} \langle 2n, 2n\rangle \quad \text{and} \quad \langle n, -n\rangle \underset{Q}{=} \langle 2n, -2n\rangle$$

to make two even (odd), so we can suppose each of f and f' has both even and odd entries. We can now use the table after Theorem 5 to arrange that f and f' can have a common term.

If $p = \infty$, the result is a corollary of Sylvester's law.

Now we come to the problem of showing that our invariants form a complete set. The following elementary proof seems to be new. It is based on a very heavy use of Witt's theorem.

We need only show that if f has *trivial invariants* (determinant a perfect square and all $[f]_v = 1$), then f is equivalent to a *trivial form* $\langle \pm 1, \pm 1, \ldots\rangle$. Using this, if g and h have the same invariants, then $g \oplus g \oplus g \oplus g$ and $h \oplus g \oplus g \oplus g$ will be equivalent to trivial forms, with the same numbers of terms of each sign by Sylvester's law, so that g and h will be equivalent by Witt's theorem. We suppose that all terms in f are square-free integers, with p the largest prime dividing any term, and show how to reduce p by adding trivial forms.

LEMMA. *If $-1 \leqslant a, b < p$, and ab is a square modulo the odd prime p, then we have $\langle atp, -btp\rangle =_Q \langle aty, -bty\rangle$ for some y with $|y| < p$.*

Proof. Write $ab = x^2 - py$ with $|x| < p/2$, so $|y| < p$. Then the equation

$$atp(b/p)^2 - btp(x/p)^2 = -bty$$

shows that $\langle atp, -btp\rangle$ represents $-bty$, and so is equivalent to $\langle aty, -bty\rangle$ by Theorem 5.

THEOREM. *A form with trivial invariants is equivalent to a trivial form.*

Proof. Using the lemma, if p is odd we have

$$\langle atp, -1, 1\rangle \underset{Q}{=} \langle atp, -btp, btp\rangle \underset{Q}{=} \langle aty, -bty, btp\rangle$$

so that to within addition of trivial forms we can replace any term atp by a corresponding term btp together with further terms involving only primes $q < p$. Since the cofactors of the p-terms (terms divisible by p) are products only of ± 1 and such primes, we can suppose all the p-terms are p or up, where $u = r + 1$ is the least positive nonresidue of p. More-

over, since $\langle p, rp\rangle$ represents up, it is equivalent to $\langle up, urp\rangle$, and so to within addition of trivial forms we can replace a pair of terms

$$(up, up) \text{ successively by } (up, urp), (p, rp), \text{ and } (p, p)$$

or vice versa, together with terms divisible only by primes less than p.

We now distinguish cases. If $p = 4k + 1$ the condition $[f]_p = 1$ implies that there are evenly many terms up, which can all be eliminated by this replacement, when we are left with evenly many terms p, by the square determinant condition. These can be replaced by pairs of terms $\langle p, -p\rangle =_{\mathbf{Q}} \langle 1, -1\rangle$ and so eliminated entirely, since -1 is a square modulo p.

If $p = 4k + 3$ we can replace terms up by $-p$ and cancel any pair $(p, -p)$, so that either all terms are p, or all $-p$. Then the condition $[f]_p = 1$ implies that the number of p-terms is divisible by four, and so since we can replace a pair (p, p) by (up, up) or vice versa, we can eliminate them all.

In this way we can decrease p until $p = 2$, when the square determinant condition tells us that there are evenly many p-terms, eliminable in pairs using the equivalences $\langle 2, 2\rangle =_{\mathbf{Q}} \langle 1, 1\rangle$, $\langle 2, -2\rangle =_{\mathbf{Q}} \langle 1, -1\rangle$, and $\langle -2, -2\rangle =_{\mathbf{Q}} \langle -1, -1\rangle$ which follow from Theorem 5. So the theorem is proved.

Other Forms of the Invariant

We have used the 4-valued version $[f]_p$ of the basic invariant only so as to ensure the multiplicative property $[f \oplus g]_p = [f]_p \cdot [g]_p$, which is essential for our proof. However, since $[a]_p \cdot [b]_p = \pm[ab]_p$, we always have $[f]_p = \pm[d]_p$, so that when we specify the determinant d, only two of the four values can arise. Most authors therefore use two-valued versions, which are often defined in terms of Hilbert's quadratic norm-residue symbol $(a, b)_p$ or $(a, b/p)$, defined to be $+1$ if the form $\langle a, b\rangle$ represents a nonzero p-adic square, and -1 if not.

It is remarkable that the Hilbert symbol can be expressed in terms of the function $[x]_p$ of a single variable x, by the formula

$$(a, b)_p = [a]_p \cdot [b]_p/[ab]_p .$$

This makes it possible to pass very easily between the function $[f]_p$ and the most common forms of the invariant, namely (in our notation):

$(f)_p = (a, b, c,...)_p = [f]_p/[d]_p$, the *exclusive Hilbert product* for f;

$(f)_p' = (a, b, c,...)_p = [f]_p \cdot [d]_p$, the *inclusive Hilbert product* for f;

$C_p(f) = C_p(a, b, c,...) = \text{sign}([f]_p)$, the *Minkowski unit* for f, (sign $= +$ for $1, i$; $-$ for $-1, -i$);

$C_p'(f) = C_p'(a, b, c,...) = \text{sign}([f]^{-1})$, the *conjugate Minkowski unit* for f.

These symbols have been used with overlapping names by various authors, so that it is wise to check their definitions when using them. If $f = \langle a_1, a_2, ... \rangle$, and $pb_1, pb_2, ..., pb_k$ are the a_i divisible by p, then

$$(f)_p = \prod_{i<j} (a_i, a_j)_p \qquad (f)_p' = \prod_{i \leqslant j} (a_i, a_j)_p$$

$C_p(f) = (X/p)$, where X is the product of $b_1, -b_2, b_3, ..., \pm b_k$, and

$C_p'(f) = (Y/p)$, where Y is the product of $-b_1, b_2, -b_3, ..., \mp b_k$.

(The last two formulas hold only for p odd, when we have also $C_p'(f) = C_p(-f)$. The Minkowski units are not usually defined for $p = 2$ or ∞.)

For general use, we recommend the invariant $(f)_p = (a, b, c,...)_p$, without any additional letter, since this is a direct generalization of the Hilbert symbol $(a, b)_p$. (The Hilbert symbol $(a, b)_p$ has certain properties which make it very natural, unlike our symbol $[x]_p$, whose properties are all enjoyed by $[kx]_p/[k]_p$ for any k.)

We add a few words about algebraic properties of the invariants. The Hilbert symbol $(a, b)_p$ is a bilinear form written multiplicatively — i.e., $(a, bc)_p = (a, b)_p \cdot (a, c)_p$, and $(1, a)_p = 1$. Theorem 2, which we do not prove here, is equivalent to the assertion that if d is specified, then there is a number x with specified values of $(d, x)_p$ for all p if and only if the product of these values over all p is 1, and $(d, x)_p = 1$ whenever d is a p-adic square. In view of the bilinearity property, this can be reduced fairly easily to the problem of finding a prime with prescribed quadratic residuacity modulo finitely many given primes, and so to the theorem that there are infinitely many primes in certain arithmetic progressions.

The function $[x]_p$ is in a sense a quadratic form written multiplicatively, for which the corresponding bilinear form is $(a, b)_p$. It enjoys, therefore, the quadratic property

$$[x]_p \cdot [abx]_p \cdot [acx]_p \cdot [bcx]_p = [ax]_p \cdot [bx]_p \cdot [cx]_p \cdot [abcx]_p,$$

which is equivalent to the bilinear property of the Hilbert symbol. But as we have pointed out, the alternative function $[\![x]\!]_p = [kx]_p/[k]_p$ (for any $k \neq 0$) also has this property.

Note added in proof. Professor M. Kneser tells me that a completeness proof similar to that described here was already known to J. Milnor, who has applied it to the equivalence problem for forms over rational function fields.

REFERENCES

BURTON W. JONES, A canonical rational form for the ring of 2-adic integers, *Duke Math. J.* **11** (1944), 715–727.

GORDON PALL, The arithmetical invariants of quadratic forms, *Bull. Amer. Math. Soc.* **51** (1945), 185–197.

O. T. O'MEARA, "Introduction to Quadratic Forms," Springer-Verlag, Berlin, 1963